#16

EV369762994

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/274,294
Filing Date 3/22/1999
Inventorship .....Gunter et al
Assignee..... Microsoft Corporation
Group Art Unit 2131
Examiner .....Taghi T. Arani
Attorney's Docket No. MS1-298US
Title: System and Method for Trusted Inspection of a Data Stream.

REPLY BRIEF TO EXAMINER'S ANSWER

To: Board of Patent Appeals and Interferences
Alexandria VA 22313-1450

From: Emmanuel A. Rivera (Tel. 509-324-9256; Fax 509-323-8979)
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Pursuant to 37 C.F.R. §1.193, Appellant hereby submits a Reply Brief to the Examiner's Written Answer for application 09/274,294. A Notice of Appeal was filed July 1, 2003. An Appeal Brief was filed on August 27, 2003. The Examiner furnished the Written Answer to the Appeal Brief on January 26, 2004.

Status of Claims

The Office in the Written Answer states claims 7-15 and 19 are allowed over the prior art. Applicants appreciate the allowance of claims 7-15 and 19.

Claims 1-6, 16-18, and 20 are currently rejected.

Therefore claims 1-6, 16-18, and 20 are pending.

Grouping of Claims

The Examiner states that

> The rejection of claims 1, 4 [group A] **and** 2, 3, 5-6, 16-18, 20 and [allowed claims] 7-15, 19 [group B] stand or fall together because Appellant's brief doe[s] not include a statement that this grouping does not stand or fall together and the reasons in support of. See 37 CFR 1.192(c)(7).

The first sentence of section 7 of Appellant's Appeal Brief provides the statement "Appellant respectfully submits that the rejected claims 1-20 do not stand or fall together". Section 7 further groups the claims into two groups, group A (claims 1, 4) and group B (claims 2, 3, 5-20). Furthermore, 37 CFR 1.192(c)(8) states that reasons in support are to be provided in the argument section. Appellant provides detailed reasons as to the support of the groupings in section 8, the argument section, of the Appellant's Appeal Brief. This is contrary to the Examiner's statement (i.e., rejection) as to the "Grouping of Claims."

Response To Examiner's Arguments

(1) The Specification Provides Full Support of the Claimed Endpoints and Intermediary.

The Examiner responds that the Appellant fails to define the claimed endpoints. The Examiner cites Intervet America Inc. v. Kee-Vet Laboratories Inc., 12 USPQ2d 1474 (CA FC 1989) "which discusses improperly construing a limitation of [a] claim not limited by its recitation in the claim nor limited in the written description"; and Bell Atlantic Network Services Inc. v. Covad Communications Group., 59 USPQ2d 1865 (CA FC 2001) "where the court affirmed summary judgment of claim construction using the specification as guidance in interpreting the claims".

Appellant does not disagree with the Examiner's interpretation of the case law; however, Appellant maintains that the specification describes three distinct entities. One embodiment in the specification describes an internal client and an external client as endpoints, and a firewall computer as the intermediary. This is contrary to the Examiner's position that a firewall computer can act as both an endpoint and as an intermediary which provides for only two distinct entities.

An embodiment describes an "external client 42 and internal client 44 establish a virtual private network connection by negotiating a session key (SK). The firewall 48 opens appropriate ports to allow the VPN key negotiation process to proceed. The key negotiation process is specific to the VPN protocol. In most key negotiation processes, the two endpoint systems (the internal and external client) use a combination of public and private keys to generate and exchange a session key." *See specification page 12, lines 14-19.* The internal client and the

external client are the two distinct endpoints – endpoints that negotiate, generate, and exchange a session key.

In this embodiment, the firewall is described as a separate intermediary that may perform inspection of the encrypted data stream that is communicated by the internal and external clients or two endpoints. The firewall performs inspection of the encrypted data stream by receiving and using the shared session key of the internal and external clients or the two endpoints. "To enable trusted data stream inspection, the firewall 48 needs to know the shared session key." *See specification page 13, lines 3-6.* "Once the firewall 48 gains possession of the session key, it can dynamically decrypt traffic in the VPN data stream between the external and internal clients, and monitor the content of the data stream." *See specification page 15, lines 9-11.*

(2) <u>The Cited Reference of Shwed Does Not Disclose an Encrypted Data Stream Transferred Between Endpoints and an Intermediary Having Access to Both Endpoints.</u>

The Examiner relies on the reference U.S. Patent 5,835,726 to Shwed et al (hereinafter, "Shwed") as disclosing firewalls that may "act[ing] as both intermediaries and endpoints". The Examiner argues that his

> broadest reasonable interpretation of claimed endpoints corresponds to Firewall 1 and Firewall 2 of Shwed acting as both intermediaries and endpoints. That is Firewall 1 and Firewall 2 both act as secure pathway for host1 and host2 as well as an intermediary to examine the data packet flowing from host 1 to host 2 or vice versa. In other words, the Firewall 1 is a source of transmitting encrypted packet(i.e. an endpoint) to intermediary firewall 2, while it is also an intermediary point for inspecting packets received from host2. The Examiner responds that Firewall 1 with respect to firewall2 is an endpoint relative to firewall1 acting as an intermediary.

Appellant disagrees. The present invention describes and claims distinctive endpoints and an intermediary. The Examiner inappropriately combines one of the firewalls described in Shwed as one of the endpoints and as an intermediary. In the Examiner's interpretation, the firewalls of Shwed are both the endpoints and the intermediaries. The client computers (i.e., host1 and host2) in Shwed are not endpoints since they do not perform or pass encrypted communication; however, in the Examiner's interpretation at least one of the client computers must be an endpoint if one of the firewalls acts as an intermediary. In other words, if host 2 is sending packets to firewall 1 which receives and inspects the packets, where firewall 1 acts as an intermediary and endpoint to host 2, then host 2 must be considered an endpoint. Shwed discloses that the client computers never encrypt the data or directly communicate with one another which the present invention particularly discloses and claims. Shwed relies on firewalls 1 and 2 to perform the communicating and encrypting. The Examiner's interpretation of Shwed provides that only the firewalls are considered as endpoints, which leads to two entities (i.e., firewall 1 and 2) encrypting data and communicating with one another, without the provision of a third entity (i.e., intermediary) to inspect the encrypted data as disclosed and recited in the claims of the present invention.

(3) The Cited Reference of Shwed Does Not Disclose the Host Computers As Endpoints.

As discussed above, in view of the Examiner's interpretation of Shwed, the host computers (i.e., host 1 and host 2) cannot be considered endpoints, since the host computers of Shwed do not negotiate, generate, and exchange a session key.

Furthermore, the host computers do not communicate an "encrypted data stream". The firewalls of Shwed perform these functions, not the host computers.

In the Examiner's arguments and scenarios that recite Shwed, a first host computer is considered an endpoint to a first firewall that is considered as a second endpoint to the first host computer. As disclosed in Shwed, unencrypted and unprotected data from the first host computer is sent to a second firewall which encrypts the data and sends it to the first firewall. Since the host computers in Shwed do not encrypt the data or negotiate, generate, and exchange a session key, the host computers can not be considered as endpoints.

As discussed above, the Examiner interprets that the firewalls of Shwed are considered as endpoints and intermediaries. This is particularly illustrated in the Examiner's rejections of claims 2, 3, 5-6 and 16-18 that "Shwed does not suggest or teach a session key known to both endpoints... The Examiner responds that Shwed's session key R is known to Firewall 1 and Firewall 2".

Therefore, in this interpretation of the Examiner, Firewall 1 and Firewall 2 are the endpoints which precludes that neither of the host computers may be endpoints.

(4) The Cited Reference of Schneier Does Not Disclose an Encrypted Data Stream Transferred Between Endpoints, an Intermediary Having Access to Both Endpoints, and Host Computers as Endpoints.

The reference Bruce Schneier, Applied Cryptography, Second Addition, 1996 (hereinafter, "Schneier") is cited by the Examiner as a secondary reference for "teaching of securely transferring the session key from one endpoint to an intermediary". However, Schneier provides no assistance as to endpoints that

transfer encrypted data streams to one another, where host computers are such endpoints.

Conclusion

Appellants further maintain their arguments as presented in the Appeal Brief filed on August 27, 2003 in support of the issues presented in the Examiner's Written Answer and issues outlined in the Apply Brief.

Appellants respectfully requests that the §102 and §103 rejections be withdrawn and that pending claims 1-6, 16-18, and 20 be allowed.

Respectfully Submitted,

Dated: 4/22/04 By: _____

Emmanuel A. Rivera, Reg. No. 45,760
(509) 324-9256